



An Imaginary Barrier

How HIPAA Promotes Bidirectional Patient Data Exchange With Emergency Medical Services

Prepared for:



By:



Contents

Overview	3
The Issue	4
Objectives.....	4
Bidirectional Sharing - More Critical Than Ever in Today's World	5
The COVID-19 Era	6
The Opioid Crisis.....	7
Emergency Triage, Treat, and Transport (ET3) Model	7
Adoption and Endorsement of Health Information Exchange	8
Federal Health IT Strategic Plan 2015-2020	8
Health Information Exchange & Emergency Medical Services (2016)	8
EMS Data Integration to Optimize Patient Care (2017)	9
Utah's Clinical Health Information Exchange.....	10
The National EMS Information System (NEMSIS)	10
How HIPAA and Federal Agencies Permit & Promote Bidirectional Patient Data Sharing.....	11
HIPAA Privacy Rule	12
Treatment Activities.....	12
Healthcare Operations Activities	13
Agency Guidance on Healthcare Operations	13
Note: OCR May Require Bidirectional Sharing in the Future	14
HIPAA Security Rule.....	15
EMS Practitioners Are Independently Required to Secure Patient Data	15
Required Safeguards for EMS Agencies	16
HIPAA Breach Notification Rule	18
What Does That Mean for Bidirectional Sharing Between EMS and Other Practitioners?	19
Conclusion	20

Overview

Page, Wolfberg & Wirth (PWW) was asked by the National EMS Information System (NEMSIS) Technical Assistance Center (TAC) to offer our opinion regarding the bidirectional sharing of patient information between Emergency Medical Services (EMS) and other healthcare providers. Many hospitals have raised concerns under the Health Insurance Portability and Accountability Act (HIPAA) about sharing of patient information with EMS, hindering EMS agencies' ability to conduct meaningful quality assurance and quality improvement of their prehospital care. This paper discusses why HIPAA does not restrict, and how the law promotes, bidirectional sharing of patient information between hospitals and EMS agencies.

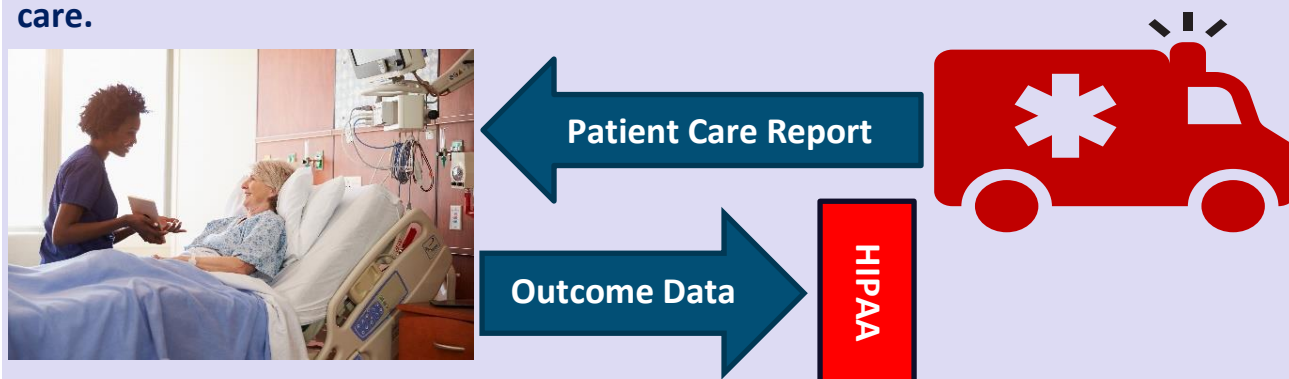
About Page, Wolfberg & Wirth

Page, Wolfberg & Wirth (PWW) is the nation's preeminent EMS, ambulance, and medical transportation industry law and consulting firm, serving hundreds of private, public, and nonprofit agencies throughout the United States. PWW's professional services encompass all of the critical issues faced by ambulance services and EMS organizations. PWW is the leading national firm when it comes to HIPAA compliance and patient privacy issues. The firm's "Ambulance Service Guide to HIPAA Compliance" and "HIPAA TV" training are the most widely used HIPAA compliance tools for EMS agencies nationwide. The ambulance industry professionals at PWW are some of the best-known and highly sought-after speakers and authors in the nation. Their presentations are featured in EMS conferences, seminars, and other events in every state in the country, and their writing has been featured in hundreds of articles, books, websites, and other publications nationally.

Additional information regarding Page, Wolfberg & Wirth is available at www.pwwemslaw.com.

The Issue

Emergency Medical Service (EMS) agencies nationwide still widely report that hospitals and other healthcare providers refuse to share patient information with them, citing concerns under the Health Insurance Portability and Accountability Act (HIPAA).¹ Misconceptions about HIPAA have created an **artificial barrier** to legitimate, approved bidirectional data exchange between EMS and other providers. As a result, many healthcare systems are missing a critical opportunity to improve patient outcomes and advance evidence-based practices in prehospital care.

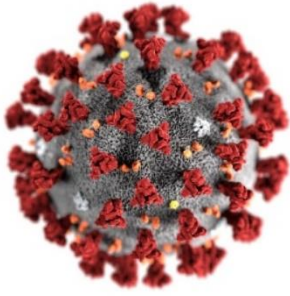


Objectives

- Establish why bidirectional sharing is critical in today's healthcare systems and how Federal agencies endorse the practice.
- Explain how the HIPAA Privacy Rule and Federal HIPAA enforcement agencies permit and promote bidirectional patient information sharing.
- Address how the HIPAA Security and Breach Notification Rules adequately address stated fears about the security of facility data.



¹ Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936).



"The recent COVID-19 pandemic underlines the importance for clinicians on the front lines to quickly access a patient's health record, regardless of where that patient previously received care."

- Dr. Neil Evans, Interim Director of the Federal Electronic Health Record Modernization

The COVID-19 Era

The COVID-19 pandemic thrust to the forefront the urgent need for hospitals and other facilities to share patient information with EMS agencies and other first responders. Shortly after the Secretary of Health and Human Services (HHS) declared a [Public Health Emergency for COVID-19](#), the Office for Civil Rights (OCR) issued a COVID-19 BULLETIN reminding healthcare providers of the many ways HIPAA permits them to share protected health information (PHI) with each other.³

On the heels of the COVID-19 BULLETIN, OCR issued significant Guidance concerning disclosures of PHI to **first responders**. This Guidance made it clear that facilities may - **and should** - share PHI with EMS agencies.⁴ The Guidance states:

"The HIPAA Privacy Rule permits a covered entity to disclose the protected health information (PHI) of an individual who has been infected with, or exposed to, COVID-19, with law enforcement, paramedics, other first responders, and public health authorities without the individual's HIPAA authorization . . ."⁵



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

**COVID-19 and HIPAA: Disclosures to law enforcement, paramedics,
other first responders and public health authorities**

OCR cited many examples of when facilities could disclose PHI to first responders under HIPAA. Significant about this Guidance, is the clear indication by OCR that facilities may share patient **outcome information** (here the infectious status of a patient) with EMS agencies under HIPAA. HIPAA not only allows the sharing of the patient's COVID-19 status with first responders, but it also permits the sharing of other types of outcome data for treatment and healthcare operations purposes.⁶

³ Office of Civil Rights, U.S. Department of Health and Human Services. (2020, February). HIPAA Privacy and Novel Coronavirus. Retrieved from <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf>.

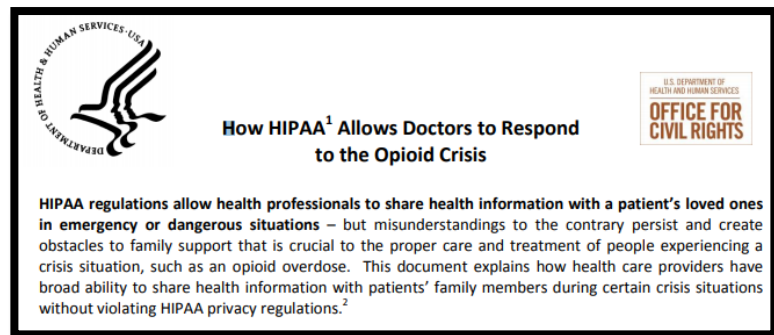
⁴ Office for Civil Rights, U.S. Department of Health and Human Services. (n.d.). COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities. Retrieved from <https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf>.

⁵Id.

⁶ 45 CFR § 164.506.

The Opioid Crisis

OCR also issued recent Guidance about how HIPAA gives healthcare providers broad authority to coordinate with each other and share necessary health information to coordinate care for opioid patients. For example, providers may inform other caregivers about a patient's opioid abuse after determining it is needed for treatment or that the patient poses a serious and imminent threat to his or her health through continued opioid abuse.

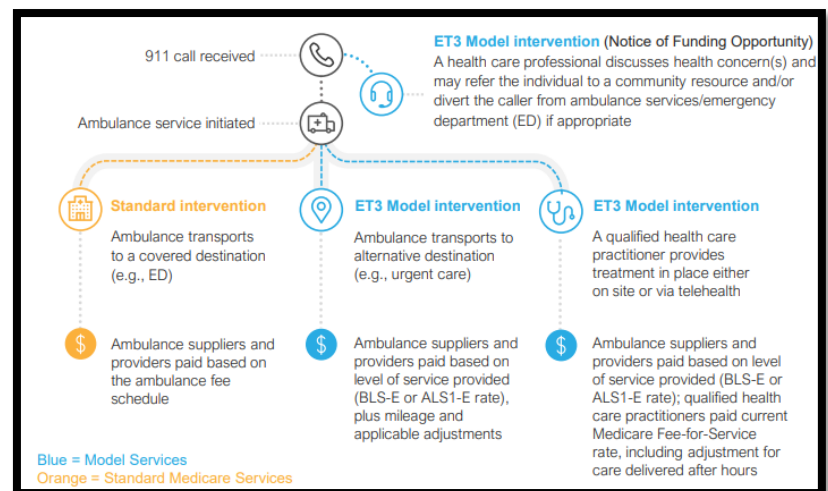


Emergency Triage, Treat, and Transport (ET3) Model

Patient information exchange between EMS and other practitioners is also critical to the success of the Center for Medicare and Medicaid Services' (CMS) Emergency Triage, Treat, and Transport (ET3) Model, announced in February of 2019.

The ET3 Model calls for participants to submit an "Interoperability Plan" that demonstrates the ability to share patient data among key stakeholders such as:

- Alternative destination sites
- Beneficiaries' self-identified routine health care providers (e.g., primary care physicians); and
- Medicare-enrolled qualified health care practitioners.⁷

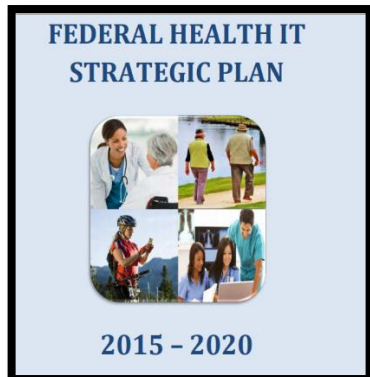


ET3 participants must demonstrate current participation in a health information exchange (HIE) or set out a plan to participate in an HIE during the model performance period. Alternatively, they must demonstrate their ability to use specific HIE standards.

The ET3 Model strives to make EMS systems more efficient by providing beneficiaries broader access to the care they need. Essential to the mission is the ability to share patient information among practitioners in EMS systems.

⁷ Emergency Triage, Treat, and Transport Model (ET3) Request for Applications (RFA); Last Modified: 05/28/2019; Available at: <https://innovation.cms.gov/files/x/et3-rfa-preview.pdf>.

Adoption and Endorsement of Health Information Exchange



Federal Health IT Strategic Plan 2015-2020

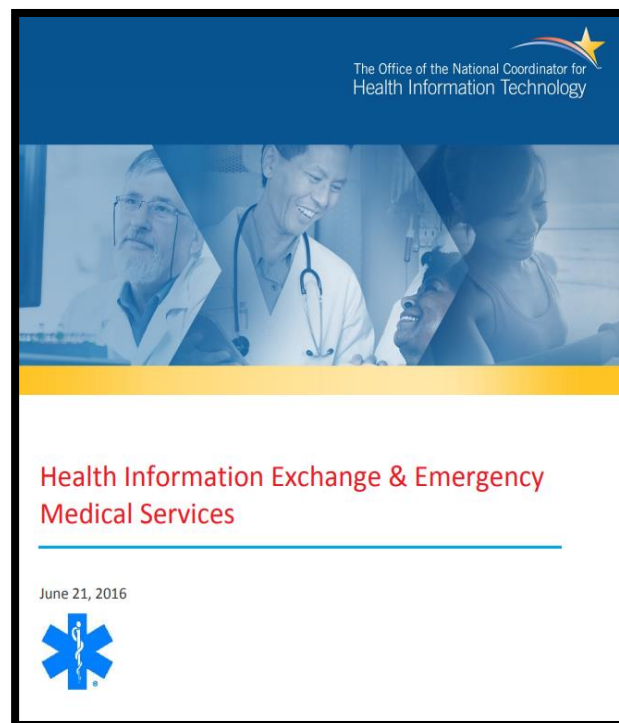
The Federal government recognized the importance of integrating EMS into Health Information Exchange (HIE) systems in **The Federal Health IT Strategic Plan 2015-2020**, stating:

“EMS practitioners provide stabilizing care and transportation services; having access to a patient’s salient clinical information as a first responder can improve patient health and safety. Access to linked outcomes data from hospitals can help EMS systems measure performance, improve their provision of care, and provide timely feedback to providers.”⁸

The Strategic Plan explains numerous situations that necessitate the sharing of information between EMS and other participants in the healthcare community.

Health Information Exchange & Emergency Medical Services (2016)

The Office of the National Coordinator for Health Information Technology (ONC) also described how EMS systems are universally regarded as an essential part of the health care system today, operating at the intersection of health care, public health, and public safety.⁹ ONC stated that the ability to use an HIE is especially critical to field paramedics because it is critical that first responders have access to relevant health data, such as medical problems, medications, allergies, and end-of-life decisions. ONC touts how the use of community paramedics charged with managing chronic conditions to reduce readmission or evaluation of non-emergency patients with alcohol, substance abuse, or behavioral health problems greatly benefit from more robust access to health information.

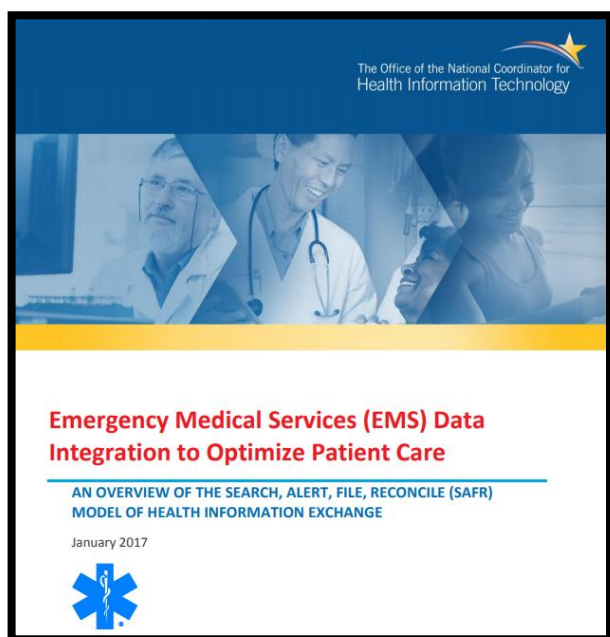


⁸The Office of the National Coordinator for Health Information Technology (ONC) Office of the Secretary, United States Department of Health and Human Services. (n.d.). FEDERAL HEALTH IT STRATEGIC PLAN 2015-2020. Retrieved from https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf.

⁹The Office of National Coordinator for Health Information Technology. (2016, June 21). Health Information Exchange & Emergency Medical Services. Retrieved from https://www.healthit.gov/sites/default/files/HIE_Value_Prop_EMS_Memo_6_21_16_FINAL_generic.pdf

EMS Data Integration to Optimize Patient Care (2017)

A 2017 Report from the ONC reveals that improving data sharing between EMS and other healthcare practitioners has already yielded significant benefits. The Report details how five EMS agencies have successfully implemented HIE/EMS initiatives using the **Search, Alert, File, Reconcile (SAFR) Model**.



	HIE Organization	Start Date of EMS-HIE Efforts	Funding Source	No. of EMS Agencies and Users with HIE Access	SAFR Elements in Use
California	San Diego Health Connect and OCPRHIO, under contract to the California Emergency Medical Services Authority (EMSA)	2013—Research and Development of SAFR Model April 2015 through July 2017—Planning and implementing a (1) San Diego /Orange County pilot and (2) an Imperial County pilot	ONC HITeCH Grant—Advance Interoperable Health Information Technology Services to Support Health Information Exchange	3	- Search, Alert, File, Reconcile to be operational in the 3 EMS agencies by July 2017 - One agency, San Diego Health Connect (an HIE organization in San Diego County) currently has an EMS hub that supports the Alert function.
Colorado	Colorado Regional Health Information Organization (CORHIO)	2014	South Metro Fire Rescue Authority—Shared cost savings model with payers, Employee Retirement Income and Security Act (ERISA), Medicaid and Self-insured Plans	1 (Operational) 6 (Implementing) 4 (Planning)	- Search - by Dispatch Health (private entity) for non-acute patients - Reconcile - by South Metro EMS
Indianapolis	Indiana Health Information Exchange (IHIE)	2004	Indianapolis Emergency Medical Services/IHIE	1 (Users: 300 EMS providers accessing HIE)	- Search
Oklahoma	MyHealth	2004—Initiative began 2010—Search ability integrated 2015—File ability integrated 2016—Re-connected to new ePCR	EMSA	3 (Users: >200)	- Search - File
Rochester	Rochester	2006—Initiative	New York Health Care	17 (covering 13)	- Alert

In 2015, the State of California Emergency Medical Services Authority (EMSA) was awarded a grant from the ONC to develop technology, infrastructure, policies, and agreements that enable interoperable HIE between multiple EMS and other healthcare practitioners. EMSA developed the Search, Alert, File, Reconcile (SAFR) model. The pilot implementations were successful, and EMSA continues to endorse the widespread integration of EMS into HIE.

EMSA established the SAFR Model to optimize bidirectional data exchange (from the HIE to the on-scene EMS practitioner, and from the EMS practitioner back to the receiving facility and the HIE). SAFR is recognized as the future of EMS patient care and the Model demonstrates how effective prehospital care is now dependent on HIE with widespread participation from all healthcare providers in local, regional, and statewide systems.

S	SEARCH	Paramedics and EMTs may look up and display patient problem list, medications, allergies, POLST and DNR in the field on ePCR screen
A	ALERT	Display patient information on hospital dashboard at ED to alert and share incoming EMS patient information to assist in time-sensitive therapies
F	FILE	Incorporate ePCR data into hospital EHR in HL7 format (using NEMESIS 3.4 CDA standards)
R	RECONCILE	Receive patient disposition information from hospital EHR to add to EMS provider patient record

Utah's Clinical Health Information Exchange

In addition to SAFR, the State of Utah's Clinical Health Information Exchange (CHIE) is a health information hub that facility and prehospital practitioners throughout Utah use to share clinical information.

CHIE is used as a bidirectional data feed, allowing EMS agencies to transmit and receive patient data. EMS agencies electronically submit patient care reports to the CHIE, and physicians within the network can then access the report information. After physicians treat or diagnose a patient, they update the patient's record on the system, where EMS practitioners can see these and any other changes to the report in near real-time.

This bidirectional flow of data allows EMS agencies to:

- Verify the accuracy of their patient assessment and treatment;
- Identify opportunities for additional education and training;
- Observe geographic and demographic trends;
- Obtain faster financial reimbursement due to accurate patient information; and
- Increase confidence in their assessment skills.¹⁰



The sharing of hospital and EMS data have already led to a demonstrable process and care improvements and has led to additional practitioner training on symptom recognition.

The National EMS Information System (NEMSIS)



NEMSIS is a national initiative managed by the Department of Transportation (DOT) National Highway Traffic Safety Administration (NHTSA) Office of EMS (OEMS) to standardize the type of data collected by EMS agencies. NEMSIS provides the framework for collecting, storing, and sharing standardized EMS data from states and territories nationwide.

A standardized system for electronic documentation and sharing of EMS data allows local agencies and State Offices of EMS to measure performance and support more effective quality improvement programs. Standardized national data have also facilitated interoperability and health information transaction. Many health information exchanges use NEMSIS standards, facilitating bidirectional exchange between EMS and other practitioners.

10 PARAMEDICS ACCESS PATIENT OUTCOME DATA – A FULL CIRCLE SUCCESS STORY. (2018, May). EMS UPDATE - Your Connections to the Office of EMS. Retrieved from <https://www.ems.gov/newsletter/may2018/Paramedics-Access-Patient-Outcomes.html>.

How HIPAA and Federal Agencies Permit & Promote Bidirectional Patient Data Sharing

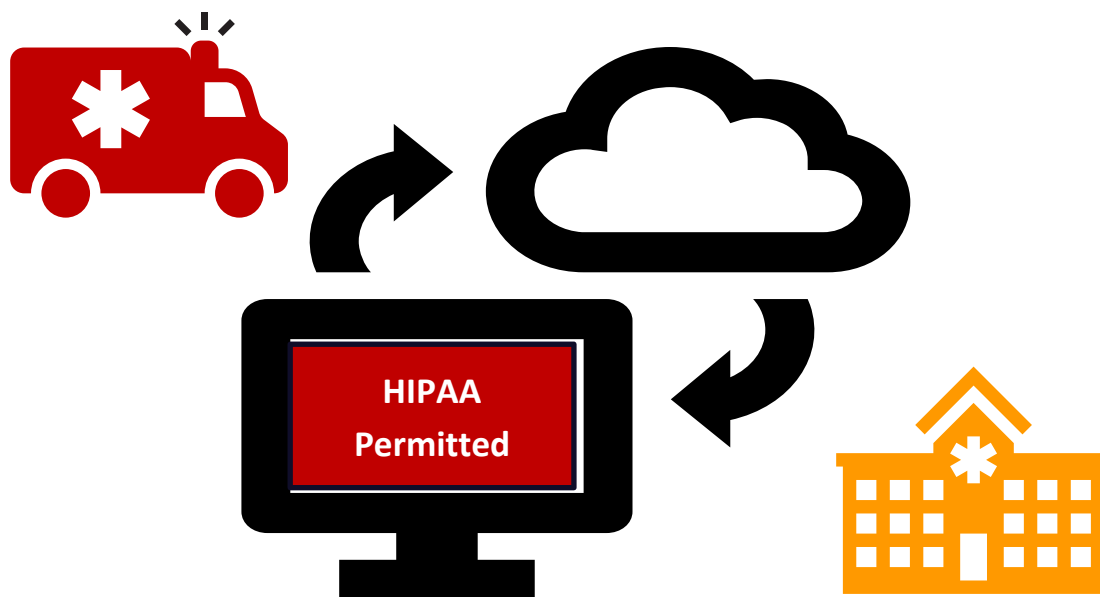
HIPAA not only permits hospitals and other practitioners to share the outcome and other patient data with EMS agencies, but the Federal agencies that enforce HIPAA unequivocally endorse the bidirectional exchange of that data.

A core aim of HIPAA is to ***“improve the efficiency and effectiveness of the healthcare system.”***¹¹ Central to measuring and improving quality in the prehospital healthcare system is analyzing outcome data from patients across the continuum of care - from prehospital treatment through hospital discharge and rehabilitation.

“Many people don’t realize that HIPAA actually enables information sharing.”

-Official Website of The Office of the National Coordinator for Health Information Technology

Hospitals (and other healthcare providers) may share patient information with EMS agencies for a host of **treatment** and **healthcare operations** activities under the HIPAA Privacy Rule. Additionally, there are ample safeguards required by the HIPAA Security and Breach Notification Rules to ensure the protection and integrity of protected health information that is shared with or accessed by EMS agencies.



¹¹Office for Civil Rights (OCR). (2017, June 16). HIPAA for Professionals. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/index.html>.

HIPAA Privacy Rule

Treatment Activities

Under HIPAA, a healthcare provider – referred to as a “covered entity”¹² – can share protected health information (PHI)¹³ with another covered entity (CE) for the treatment activities of that other provider, without patient consent or authorization.¹⁴

Treatment is broadly defined as:

“The provision, coordination, or management of health care and related services by one or more providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for care from one provider to another.”¹⁵

OCR issued Guidance, making it clear that EMS practitioners are providing “treatment” within the meaning of HIPAA when exchanging healthcare information with providers involved in the patient’s care.¹⁶ **As such, disclosures or transmissions of patient information to or from other providers are permissible without the need to obtain patient consent.**

According to joint Guidance from ONC and OCR, the term treatment also means prospective **future** treatment activities.¹⁷ This means EMS agencies may participate in HIE arrangements and utilize an HIE to exchange patient information for HIPAA-permitted activities, such as treatment.



¹² A covered entity is generally any healthcare provider who transmits healthcare claims to a health plan or government payer (such as Medicare or Medicaid). 45 CFR § 160.103.

¹³ PHI is defined as any individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity. Id.

¹⁴ 45 CFR § 164.506(c)(2).

¹⁵ 45 CFR § 164.501.

¹⁶ HHS, When an ambulance service delivers a patient to a hospital, is it permitted to report its treatment of the patient and patient's medical history to the hospital, without the patient's authorization? (2002). <https://www.hhs.gov/hipaa/for-professionals/faq/273/when-an-ambulance-delivers-a-patient-can-it-report-its-treatment-without-authorization/index.html#:~:text=Yes.,provider's%20treatment%20of%20the%20individual>; See also, 45 Code of Federal Regulations (CFR) 164.506.

¹⁷ U.S. Department of Health and Human Services, Office for Civil Rights. (2016, January). Permitted Uses and Disclosures: Exchange for Treatment. Retrieved from https://www.healthit.gov/sites/default/files/exchange_treatment.pdf.

Healthcare Operations Activities

A covered entity can also share PHI with another covered entity (CE) for the **healthcare operations activities** of the other CE without needing patient authorization.¹⁸ Healthcare operations¹⁹ activities include:

Conducting quality assessment and improvement activities
Developing clinical guidelines
Conducting patient safety activities as defined in applicable regulations
Conducting population-based activities relating to improving health or reducing health care cost
Developing protocols
Conducting case management and care coordination (including care planning)
Contacting health care providers and patients with information about treatment alternatives

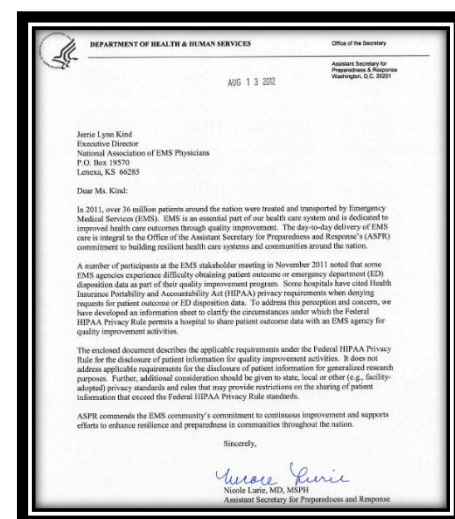
Generally, before a CE can share PHI with another CE for a healthcare operations reason: (1) both CEs must have or have had a relationship with the patient (can be a past or present patient); (2) the PHI requested must pertain to the relationship; and (3) only the **minimum information necessary** for the health care operation at hand should be disclosed.

When the requesting party is a covered entity, HIPAA permits the entity receiving the request to rely on the judgment of the party making the request for purposes of complying with the minimum necessary standard. For example, a hospital may rely on an EMS agency's request for all hospital outcome data as constituting the minimum amount of PHI that is needed by the EMS agency, and the hospital would be in compliance with the minimum necessary standard if it provided all outcome data to the EMS agency.

Agency Guidance on Healthcare Operations

In 2012, the Department of Health and Human Services (HHS) Assistant Secretary for Preparedness & Response (ASPR) issued a letter to the National Association of EMS Physicians outlining that HIPAA permits the sharing of outcome data with EMS agencies. This letter was written in response to EMS stakeholders voicing difficulty in obtaining patient outcome data as part of their quality improvement program.

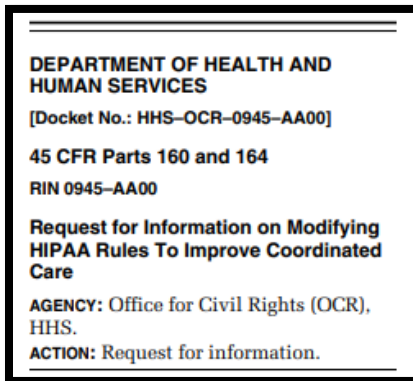
The letter states HHS's position that: "Hospital[s] may share patient health outcome information with the EMS practitioner for certain health care operations activities of the EMS practitioner, such as quality improvement activities, as long as both entities have (or have had in the past) a relationship with the patient in question."



¹⁸ 45 CFR 164.506(c)(4).

¹⁹ 45 CFR § 164.501.

Note: OCR May *Require* Bidirectional Sharing in the Future



Current HIPAA regulations permit information sharing between healthcare providers for a wide variety of reasons, including coordinating care and conducting follow-up healthcare operations activities. But healthcare providers are still not sharing PHI in many instances because of misconceptions about HIPAA.

OCR is contemplating issuing new rules to encourage and incentivize providers to share patient information by amending the regulations to **require** healthcare providers to share PHI with each other for treatment, payment, and healthcare operations purposes. This is a clear indication that OCR strongly endorses bidirectional

sharing of PHI among providers and that it is closely considering such a requirement.

What Does That Mean for Bidirectional Sharing Between EMS and Other Practitioners?

Active and Future Treatment

When EMS practitioners and facility providers are actively treating the patient, they can communicate whatever information is necessary to coordinate healthcare for the patient. So, an ambulance service that delivers a patient to a hospital can share information pertaining to the care the patient received and the patient's medical history with the hospital. Similarly, the hospital may share any pertinent medical information it has concerning the patient with the ambulance service necessary to coordinate ongoing care. If the patient were being transferred to another facility, the originating facility can share treatment information with the EMS agency doing the transfer because that agency would need to know that information to properly care for the patient during the transfer.



HIPAA also permits hospitals (and other facilities) to share PHI with EMS agencies about the patient's treatment, the patient's outcome, and the discharge diagnoses or summary condition of the patient so that ambulance services can provide appropriate treatment if and when they encounter the patient in the future. EMS agencies are permitted by HIPAA to access this information if they treat the patient in the future. This is a hallmark of health information exchange – practitioners access stored, combined medical information on an as-needed basis for their treatment needs.

Healthcare Operations

In addition, when an EMS agency transports a patient to a facility, that facility may provide health information to the EMS agency for any healthcare operations of the EMS agency. For example, if the EMS agency conducts clinical QA/QI on patients transported to a hospital, the hospital may provide outcome and disposition data to the EMS agency for the clinical QA/QI program. Both covered entities (the EMS agency and the hospital) had a relationship with the patient, and the PHI provided pertains to that relationship.

HIPAA Security Rule

ADMINISTRATIVE SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
Emergency Access Procedure	(R)		
Automatic Logoff	(A)		
Encryption and Decryption	(A)		
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
Encryption	(A)		

EMS Practitioners Are Independently Required to Secure Patient Data

A significant concern that hospitals articulate about sharing the outcome with EMS agencies is that the information will not be properly secured by those agencies. This concern is assuaged by the fact that EMS agencies are required to employ their own safeguards for PHI that they receive from other healthcare providers. Moreover, discussed in the Breach Notification section below, generally, hospitals are not responsible for the breaches of EMS agencies.

All covered entities - including EMS agencies - must implement all of the standards under the HIPAA Security Rule's administrative, physical, and technical safeguards. That means EMS agencies must have in place the same (or roughly the same) safeguards that hospitals are required to employ. And EMS agencies are subject to penalties from HHS if they fail to comply with the Security Rule, just like hospitals. Therefore, there are no greater risks for hospitals sharing PHI with EMS agencies than there are with the EMS agencies providing their PHI to the hospitals, as they routinely do when they transfer care upon arrival.



The safeguards that hospitals and EMS agencies are required to implement are designed to ensure that PHI that is shared among and between healthcare providers is secure while being created, accessed, maintained, and transmitted.

Required Safeguards for EMS Agencies

- **Role-Based Access.** The Security Rule requires covered entities to implement policies and procedures for authorizing access to electronic PHI (“e-PHI”) only when such access is appropriate based on the user or recipient's role (role-based access).²⁰ That means that an EMS agency is required only to grant access to another provider’s data to individuals who need access to that information. That includes outcome information on a hospital’s system, the information in an HIE and any information received and maintained on the EMS agency’s information network. 
- **Workforce Authorization, Training, and Sanctions.** Covered entities must provide for appropriate authorization and supervision of workforce members who work with e-PHI.²¹ Healthcare providers must train all workforce members on their security policies and procedures,²² and they must have and apply appropriate sanctions against workforce members who violate their policies and procedures.²³ EMS agencies must train workforce members regarding appropriate access to PHI - including other providers’ data - and they are required to discipline employees who inappropriately access, use, or disclose that information. For example, EMS practitioners who are credentialed as read-only users on a hospital’s database must be trained that they should only access the information they need to perform job-related functions, such as conducting QA/QI. Staff members who “snoop” on records or inappropriately access PHI must be sanctioned just as a hospital would be required to sanction one of its own employees if he inappropriately “snooped” on a medical record. 
- **Workstation and Device Security.** A covered entity must ensure the security of workstations and electronic media.²⁴ That means EMS agencies must have policies concerning how its workforce members use workstations and other devices so workforce members do not inappropriately use those devices. 

²⁰ 45 C.F.R. § 164.308(a)(4)(i).

²¹ 45 C.F.R. § 164.308(a)(3) & (4).

²² 45 C.F.R. § 164.308(a)(5)(i).

²³ 45 C.F.R. § 164.308(a)(1)(ii)(C).

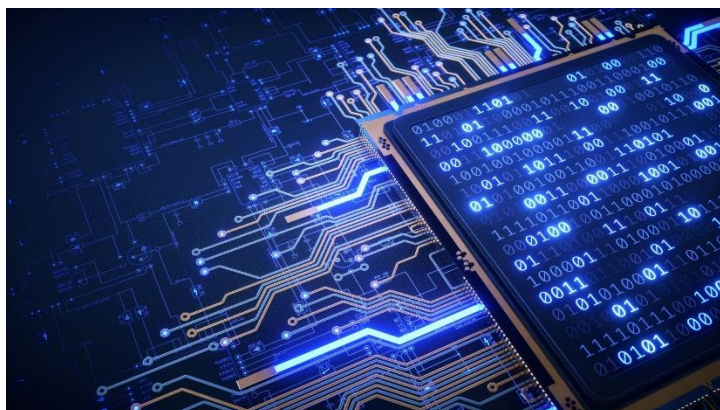
²⁴ 45 C.F.R. §§ 164.310(b) & (c).



- **Access Control.** Covered entities must implement policies and procedures that allow only authorized persons to access e-PHI.²⁵ So, EMS agencies must implement protections such as **unique user IDs, secure passwords, automatic logoffs**, and other safeguards that ensure only authorized workforce members access PHI, including PHI from other healthcare providers.



- **Audit Controls.** Covered entities must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.²⁶ All access to PHI, including outcome data must be tracked and examined by EMS agencies. In addition, hospitals are required to track access within their databases and would have the ability to audit access by any EMS agency workforce member who was provisioned access to the system.
- **Integrity Controls.** Covered entities must implement measures to confirm that e-PHI has not been improperly altered or destroyed.²⁷ EMS agencies have a duty to ensure their workforce members do not alter or destroy any PHI to which they have access (including data of other providers).
- **Transmission Security.** Covered entities must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.²⁸ EMS agencies would be required to consider encryption whenever transmitting PHI. A hospital is also responsible for disclosing PHI to a receiving EMS agency in a permitted and secure manner.



²⁵ 45 C.F.R. § 164.312(a).

²⁶ 45 C.F.R. § 164.312(b).

²⁷ 45 C.F.R. § 164.312(c).

²⁸ 45 C.F.R. § 164.312(e).

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule states that the covered entity maintaining the PHI (in any form) when a breach occurs is the organization that bears breach notification responsibility under HIPAA.²⁹ Therefore, once PHI is received by an EMS agency, any breach of that PHI becomes the responsibility of the EMS agency. Hospitals are generally not responsible for improper uses, disclosures, security incidents, or breaches of PHI by an EMS agency. The only thing the hospital is responsible for is ensuring that it provides the PHI to the EMS agency in compliance with HIPAA (*i.e.*, securely).

Under HIPAA, PHI is defined as individually identifiable information that is created or **received** by a healthcare provider.³⁰ So, PHI received from another healthcare provider becomes PHI of the receiving provider, and the receiving provider may only use and disclose the PHI in accordance with HIPAA. This is true even if the PHI was mistakenly or inappropriately received by the healthcare providers. Once PHI is in the possession of a HIPAA covered entity, the information must be protected in the same manner as PHI that the covered entity created.

Joint Guidance from ONC and OCR makes it clear that: (1) each healthcare provider (covered entity) is responsible for its uses and disclosures; and (2) a covered entity that compliantly discloses PHI to another covered entity is not responsible for subsequent uses and disclosures of the PHI it discloses. Below is an illustration, from joint ONC and OCR Guidance, depicting a hospital sharing PHI with a physician's office for treatment:

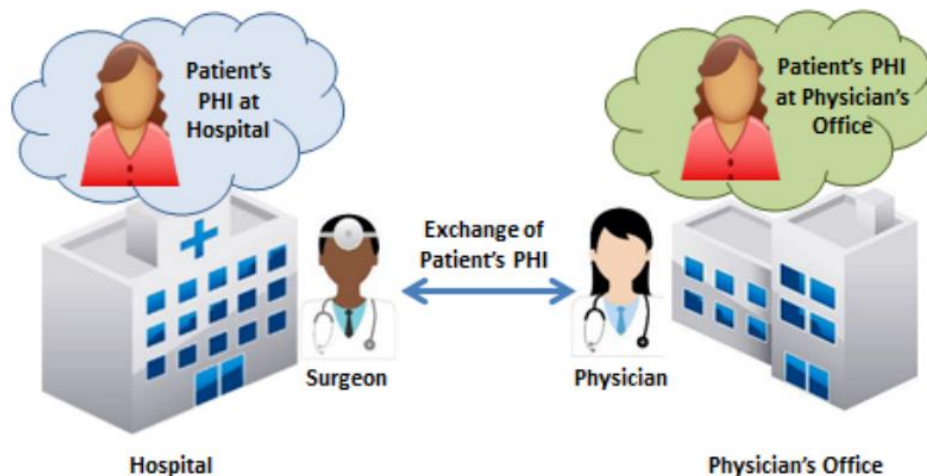


Figure 1: Hospital and Treating Physician exchange information scenario

²⁹ 45 CFR § 164.400 et. seq.

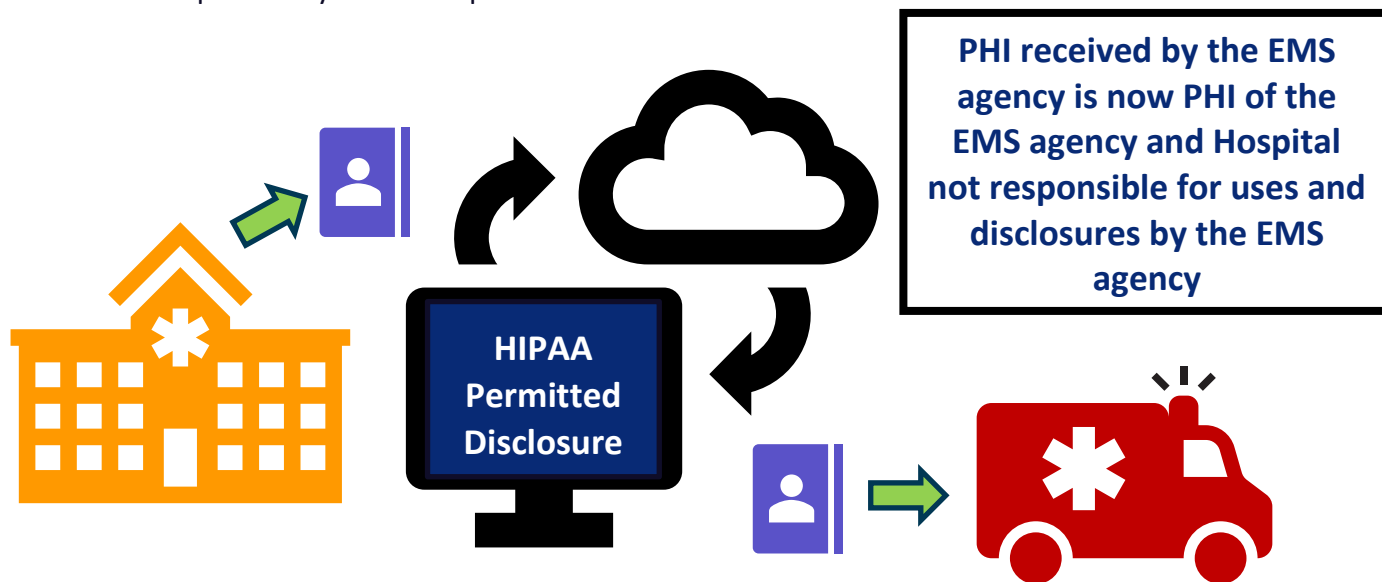
³⁰ 45 CFR § 160.103.

Regarding the illustration, the Guidance provides:

“A common question that arises is whether, in the above illustration, the disclosing hospital will be held responsible under HIPAA for what the receiving provider does with the PHI once the hospital has disclosed it in a permissible way under HIPAA. For example, what if the receiving physician experiences a breach of the PHI? Under HIPAA, after the receiving physician has received the PHI in accordance with HIPAA, the receiving physician, as a CE itself, is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to subsequent uses or disclosures or any breaches that occur. The disclosing hospital is responsible under HIPAA for disclosing the PHI to the receiving physician in a permitted and secure manner, which includes sending the PHI securely and taking reasonable steps to send it to the right address.”³¹

What Does That Mean for Bidirectional Sharing Between EMS and Other Practitioners?

If a hospital provisioned secure access to its patient database or securely transmitted PHI to an EMS agency for treatment or quality assurance activities of the EMS practitioner, the hospital would generally not be responsible for any improper uses and disclosures – including any breaches – of the PHI. After the receiving EMS agency received the PHI in compliance with HIPAA, the receiving EMS agency, as a covered entity, is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to subsequent uses or disclosures or any breaches that occur. Any breach would be the responsibility of the EMS agency that received the PHI just as a breach by a hospital of its PHI – including an EMS patient care report that becomes part of the hospital’s records – would be the responsibility of the hospital.



³¹ See, Guidance from the Office of the National Coordinator for Health Information and Technology and the U.S. Department of Health and Human Services Office for Civil Rights, Permitted Uses and Disclosures: Exchange for Treatment (January 2016), Available at https://www.healthit.gov/sites/default/files/exchange_treatment.pdf.

Conclusion

While there may be obstacles that remain for bidirectional sharing of patient information, HIPAA is not one of them. Not only does HIPAA permit other healthcare providers to share PHI with EMS agencies, but the law also endorses bidirectional sharing for treatment and healthcare operations. HIPAA also requires EMS agencies to safeguard the PHI that they receive from hospitals in the same way that hospitals must protect their own PHI.

Sharing patient information not only benefits EMS agencies, but it improves the prehospital care by revealing evidence-based practices that make a difference for patients in the field. It also reinforces to EMS practitioners that the care they provide is meaningful and effective.